Management Should Take Action to Address Employees' Personal Use of E-Mail

November 2000

Reference Number: 2001-20-017

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

November 21, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Management Should Take Action to Address Employees' Personal Use of E-Mail

This report presents the results of our review of management controls for ensuring that employees do not misuse the Internal Revenue Service's (IRS) e-mail system.

In summary, we found that while the use of e-mail as an effective business tool is to be encouraged, there is strong evidence that employee use of e-mail for non-business purposes appears significant. Non-business use occurred because the IRS had not implemented policies on e-mail usage until recently and still has not developed practices for enforcing the policies.

We recommended that the Chief Information Officer develop procedures to enforce a recently issued policy informing employees of unacceptable non-business use of e-mail. Employees should be educated on the risks and costs associated with non-business e-mails. Also, the Chief Information Officer should evaluate available e-mail scanning software and implement a monitoring system to identify the extent of employee unauthorized use of e-mail.

Our recommendations will help IRS reduce the negative impact of non-business use of e-mail on productivity and telecommunications traffic. In addition, the risk will be reduced of creating potentially hostile work environments caused by inappropriate or offensive e-mail.

Management's response was due on November 1, 2000. As of November 14, 2000, management had not responded to the draft report.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions, or your staff may contact Scott Wilson, Associate Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Executive Summary

E-mail use for business purposes is escalating rapidly as government and private industry increasingly recognize that electronic messaging is faster and cheaper than more traditional methods of communication. Increased use of e-mail as an effective business tool should be encouraged within an organization because many benefits, such as more rapid and accurate communication, accrue due to its use. Along with the benefits, come some risks. While some are widely known, such as the potential spread of computer viruses, others may also lead to negative consequences. Non-business use of e-mail is among these risks. The Internal Revenue Service (IRS) currently has approximately 70,000 computers that can transmit and receive e-mail and will soon almost double this number. We conducted this review to determine whether management had adequate controls for ensuring that employees do not misuse the IRS e-mail system.

Results

Although e-mail records maintained by the IRS and the Treasury Department were limited, we identified strong evidence of significant non-business use of e-mail by IRS employees. In our opinion, management needs to take action to limit the non-business use of e-mail.

Employee Non-Business Use of E-Mail Appears Significant

Approximately 47 percent of the 82,000 incoming e-mails we reviewed were for non-business purposes. These e-mails had been sent to IRS employees from outsiders and ranged from an online travel magazine to an address providing daily jokes. For example, we identified 1 employee who received 1,151 messages from a "Shared Parenting" organization. Another individual received 450 e-mails from a high school alumni group, while another had 84 messages from a group connected to a popular rock singer.

Due to limitations in the data and difficulty in identifying certain addresses, we could not determine whether e-mails were for business or non-business use for another 47 percent of the incoming e-mails. We considered only six percent of the e-mails as clearly business related since the messages were from sites that provided financial, computer and tax related information. Even though employees cannot always control e-mail received from outsiders, the effect these e-mails are having on productivity, telecommunications capacity, and the potential spread of computer viruses should be addressed.

While data were not available to analyze the addresses of outgoing messages for non-business use, we noted certain e-mail usage that appeared questionable because of the number of messages sent. For example, we identified 1 employee who sent

26,000 messages and another who sent over 13,000 messages during the 75 workdays we reviewed. We were unable to review e-mail sent between IRS employees because the IRS had no standard e-mail storage procedures and the messages were not available for review.

The true extent and effects of non-business e-mails were not known because the IRS did not maintain cost data for telecommunications capacity dedicated to e-mail. However, because of the high number of non-business e-mails in our limited sample and examples from the private sector, we believe the impact on productivity and telecommunications capacity could be significant. The IRS could also be exposed to computer viruses transmitted by e-mail and to lawsuits if e-mail messages contain inappropriate or offensive material.

Management had not yet implemented government and industry recommendations for controlling e-mail misuse by employees. The Technology Security Committee, chaired by the Chief Information Officer, recently issued a policy to employees on the use of all electronic communication, including e-mail. Previously, emphasis had not been placed on the need to use e-mails for business purposes only. Procedures are still needed to enforce the policy.

Summary of Recommendations

Actions are needed to identify the extent of inappropriate use of e-mail and to curb the use of non-business e-mails to improve productivity and reduce telecommunications costs. The Chief Information Officer should follow the lead of many in the private sector and develop controls and procedures to enforce the policy prohibiting the use of non-business e-mails. While we recognize that monitoring employees' e-mails is sensitive due to privacy concerns, management should implement a system to ensure compliance with the recently issued electronic communication policy and emphasize to employees the effects of unauthorized e-mails.

Management's Response: Management's response was due on November 1, 2000. As of November 14, 2000, management had not responded to the draft report.

Objective and Scope

Our objective was to determine whether controls over employee use of e-mail were adequate.

Our objective was to determine whether management had adequate controls for ensuring that employees do not misuse the Internal Revenue Service (IRS) e-mail system. To accomplish this objective we reviewed IRS, federal, and industry policies, guidelines, and procedures for ensuring that employees do not use e-mail systems for transmitting personal or inappropriate messages.

We could not readily access and review the IRS' electronic records containing the contents and titles of e-mail messages sent from employee to employee. Instead, we analyzed data on 1.9 million e-mail messages contained in a Treasury Department log that included messages sent to and received from non-employees between January 1, 2000, and April 19, 2000. Since the log contained neither message content nor the title of the message, we researched the address of the external party using the Internet and made reasonable conclusions as to whether messages were business-related.

The audit was conducted primarily at the National Headquarters. Several IRS field personnel were contacted to include their perspective and responsibilities. The audit was performed between February and May 2000 in accordance with *Government Auditing Standards.*

Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

Background

The use of e-mail is increasing rapidly in both government and industry. Electronic messaging is faster and cheaper than more traditional methods of communication. Increased use of e-mail as an effective business tool should be encouraged within an organization because many benefits, such as more rapid

and accurate communication, accrue due to its use. While e-mail offers the benefits of speed and efficiency, it also presents management with new risks. Recent articles and studies[1] indicate that employee misuse of e-mail could be significant. These sources estimated that at least 50 percent, and as much as 90 percent, of employee e-mail was for non-business use.

Non-business use of e-mail can account for a substantial amount of e-mail usage.

Federal guidelines state agencies should control the use of e-mail, which could include monitoring.

Several National Institute of Standards and Technology publications recommend that agencies issue specific policies on e-mail usage, privacy, and monitoring, and that employees be trained in them so that violations can be discouraged. Guidance issued by the Chief Information Officers' Council states that agencies should have controls to ensure compliance with their e-mail policies, which could include monitoring.

Office of Management and Budget Circular A-130 requires that users of computer systems that connect to the Internet be given written rules of behavior, including the consequences for noncompliance, and training on the rules. The Treasury Security Manual states that employees should not (1) send or encourage receipt of non-business messages, (2) subscribe to material not related to official business, and (3) conduct official business on accounts with Internet service providers.

---

[1]Lisa Guernsey, "You've Got Inappropriate Mail; Monitoring of Office E-Mail Is Increasing," *The New York Times*, April 5, 2000.

Martin Oxley, "Private Use of E-Mail Costs Companies Big Bucks," *Marshall Software News*, May 22, 1998.

Paul Verdon, "Protection and Control for E-Mail Developed," *Marshall Software News*, April 2, 1998.

TenFour US Inc., *Five Keys to Successfully Protecting Your E-Mail*, 1999.

Elron Software Inc., 1999 *E-Mail Abuse Study*.

Results

Management needs to implement various controls over employee use of e-mail.

Although records maintained by the IRS and the Treasury Department for e-mails were limited, we identified strong evidence of non-business use by employees. In our opinion, management needs to take action to limit the non-business use of e-mail.

Unless the IRS takes action, the loss of productivity and increase in telecommunications costs caused by such misuse could become more significant. The IRS currently has approximately 70,000 computers that can transmit and receive e-mail and will soon almost double that number.

Employee Non-Business Use of E-Mail Appears Significant

For the purposes of our audit, we attempted to determine the extent of non-business use of e-mails sent between employees over the IRS network, e-mails sent by employees to non-employees, and e-mails received from non-employees.

Sufficient data were not available to determine the extent of non-business use of e-mail sent between employees.

Employee to Employee E-mail

E-mails sent between employees accounts for the majority of messages sent over IRS telecommunications lines. We were unable to review internal e-mail for non-business use because the IRS had no standard e-mail storage procedures and the messages were not readily available for our review.

Outgoing E-Mail to Non-employees

About 1.6 million (84 percent) of the 1.9 million messages on the Treasury Department log we reviewed were outgoing messages to non-IRS addresses. We could not determine whether these messages were for business or non-business because the log did not contain the contents or titles of the messages, nor the address of the outside party.

While we could not analyze the addresses of outgoing messages for non-business use, we noted certain e-mail usage that appeared questionable because of the volume of messages sent.

The volume of outgoing messages indicates potential misuse.

For example, we identified 1 employee who sent 26,000 messages and another who sent over 13,000 messages during the 75 workdays covered by the log and included in our sample period. Thirty-eight employees had volumes of messages ranging from 2,000 to 8,500 messages each during the same period.

Incoming E-Mail from Non-employees

The remaining 300,000 messages in the 1.9 million record log came into the IRS from outsiders. We reviewed approximately 82,000 of them that clearly identified the address of the party who had sent them. We identified those senders of the 82,000 messages who had sent over 100 messages to IRS employees during the 75 workdays covered by the log. This sample represented 92 percent of the 82,000 messages. Since the Treasury log contained neither message content nor the title, we researched the address of the sender and the sender's organization to make a reasonable conclusion as to whether the messages were business-related.

Due to the limited address data provided by the logs and our inability to find some of the addresses, we could not determine the purpose of the message for 47 percent of the 82,000 messages. We determined that six percent of the messages were for business use, since the messages were from sites that provided financial, computer, and tax-related information.

Approximately 47 percent of incoming e-mail were non-business related. For example, 1 employee received 1,151 messages from a "Shared Parenting" organization and 47 additional messages from another organization called "Dads Talk." Another individual received 450 messages from a high school alumni group, while another employee had 84 messages from the address of a popular rock singer. Other addresses that indicated non-business use ranged from an online travel magazine to an address providing daily jokes.

We believe it is likely that misuse could also be occurring in the messages we did not review. Even though employees cannot always control non-business e-mails from non-employees, it is reasonable to believe that IRS employees encouraged at least some of it. Significant non-business use has also been reported in the private sector.

Non-business use of e-mail can have a significant impact on productivity and telecommunications capacity.

Non-business use of e-mail can have a significant effect on telecommunications capacity. The true extent and effects of non-business e-mails were not known because the IRS did not maintain cost data for telecommunications capacity dedicated to e-mail. However, Internet e-mail consumes a large portion of the IRS' telecommunications capacity and is growing as fast as any other communication protocol. According to data we obtained from the IRS' Telecommunications Management Center, Internet e-mail consumed about 62 percent of the IRS' capacity for traffic during the 6-week period starting February 21, 2000, and ending April 3, 2000.

The use of e-mail for non-business purposes can also affect productivity. A study by the surfCONTROL division of JSB Software Technologies plc. [2] showed that the annual cost of non-business Internet browsing for one hour a day was approximately $14,000 per employee. Equivalent information was not available for non-business use of e-mail due mostly to the fact that it was difficult to estimate how much time employees spend on these messages. We concluded, however, that non-business use of e-mail can have a similar impact on productivity as non-business Internet browsing.

Employees who use e-mail for non-business purposes risk spreading harmful computer viruses. According to industry estimates, between 65 and 90 percent of viruses are transmitted via e-mail.[3]

---

[2] surfCONTROL, *The Cost of Non-Business Browsing: An Illustration, 1999.*

[3] Heather Harreld, "Antivirus Software Covers The Perimeter," *Federal Computer Week*, April 10, 2000.

In addition, employees who received e-mail with objectionable content have filed sexual harassment and discrimination suits against major private sector employers, and courts have held companies financially liable to employees. We know of no IRS employees who have filed suits. However, based on employee complaints, the IRS identified 44 cases of e-mail misuse between December 1998 and March 2000. These cases all resulted in investigations being conducted by the Treasury Inspector General for Tax Administration Office of Investigations because the complaints stated that the messages contained inappropriate or offensive content.

The IRS did not have a sound, enforceable e-mail policy.

We believe that employee misuse occurred because the IRS did not have, until recently, policies governing e-mail use. However, the Technology Security Committee, chaired by the Chief Information Officer, issued a policy in June 2000. It still has not developed practices for enforcing the policies. In addition, the IRS did not train employees on the liability and security risks that misuse of e-mail present.

The IRS did not monitor e-mail so it could not determine the extent that employees were using e-mail for non-business purposes, and the related costs. Without such data, the IRS would not be aware of the impact misuse might be having on productivity, the unnecessary consumption of system resources, and the exposure to liability and security breaches.

Even if the IRS had a system for monitoring e-mail, it would have difficulty enforcing the policy because it does not uniformly archive e-mail. We contacted officials responsible for 10 of the 46 computers that manage the e-mail databases nationwide about their practices for archiving e-mail messages. We received responses that ranged from 1 individual who claimed no responsibility for archiving e-mail messages to a coordinator who stated that e-mail tapes were retained for 1 year.

To control employee e-mail misuse, security consultants recommend that organizations formulate e-mail policies to inform employees of unacceptable practices and then

monitor e-mail to enforce such policies. One recent survey found that almost 60 percent of corporate employers had e-mail policies.[4] A survey by the American Management Association[5] reported that the percentage of employers that store and monitor employee e-mail has grown from about 15 percent in 1997 to about 38 percent in 2000. While we recognize that there are privacy concerns associated with monitoring e-mail, employees do not have the right or expectation of privacy while using Government e-mail at any time.[6]

Review of employee e-mail is becoming a necessary part of managing an e-mail system.

A recent article in *The New York Times*[7] reported that hundreds of companies are reviewing employee e-mail on a routine basis. Numerous vendors offer software capable of scanning e-mail contents and attachments. Most monitoring software can intercept messages with questionable content and delete them or let an administrator decide what to do with them. One vendor provides software that can scan messages for "strings." These can be single words or phrases that, once identified, are flagged for some action by the administrator. Other software verifies From, Sender and Subject fields, to alert a manager to possible unauthorized e-mail messages.

---

[4] Federal CIO Council, General Services Administration, "*Limited Non-business Use of Government Office Equipment Including Information Technology,"* May 19, 2000.

[5] American Management Association, *2000 AMA Survey, "Workplace Monitoring & Surveillance, Summary of Key Findings."*

[6] General Services Administration, Website, *Personal Use Policies, Limited Non-business Use,* May 2, 2000.

Smith v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa., 1996).

[7] Lisa Guernsey, "You've Got Inappropriate Mail; Monitoring of Office E-Mail Is Increasing," *The New York Times*, April 5, 2000.

Recommendations

The Chief Information Officer should follow the lead of many in the private sector and develop controls and procedures to enforce the policy prohibiting the use of non-business e-mails. Specifically:

1. The Chief Information Officer should develop procedures to enforce the policy that was recently issued informing all employees of unacceptable non-business use of e-mail. The procedures should state that e-mail messages will be periodically monitored to ensure compliance with the policy. Chief Counsel and Labor Relations should also be involved in developing these procedures, particularly in deciding disciplinary actions for offenders. In addition, employees should be educated on the risks and costs associated with non-business e-mails.

2. The Chief Information Officer should evaluate available e-mail scanning software and implement an e-mail monitoring system to assist in identifying the extent of employee unauthorized use of e-mail. Standard procedures for maintaining e-mails are necessary to ensure the effectiveness of the monitoring system.

Management's Response: Management's response was due on November 1, 2000. As of November 14, 2000, management had not responded to the draft report.

Conclusion

We believe that the impact of employee non-business use of the IRS e-mail system could be significant based on the limited sample we reviewed and on the results of studies conducted in the private sector. Management needs to implement controls to deter and detect employee misuse of the e-mail system. Actions are also needed to raise employee awareness and to monitor e-mail.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective was to evaluate the usage of the e-mail system and determine whether management had adequate controls for ensuring that employees do not misuse the Internal Revenue Service (IRS) e-mail system. To accomplish this objective, we:

I. Evaluated, to the extent possible, IRS e-mail usage to determine that e-mail is accessed for official use only. We attempted to identify the level and cost associated with non-business usage. We identified adherence to current access policies and evaluated controls to measure and monitor that adherence.

A. Attempted to obtain and assess the contents of current e-mail usage policy and guidelines from Information System's Security, Evaluation and Oversight for adequacy and consistency with Treasury guidelines.

B. Obtained all relevant information from telecommunications managers and/or staff to determine current and anticipated e-mail usage and capacity. Determined whether plans existed to provide e-mail access to more employees in the future.

C. Obtained all necessary information from the project manager of the Enterprise Messaging Stabilization and Expansion project to identify program cost, system capacity, security implications, and implementation time frames.

D. Determined how many computers manage the e-mail databases in the IRS and where they are located. Determined the archiving requirements for those computers that would facilitate any monitoring activities.

E. Determined whether there were procedures in place to monitor e-mail usage activities, such as capturing information on e-mail traffic, reviewing files on e-mail computers or workstations, or using software to scan the content of e-mail on the network. Attempted to identify the reasons that the IRS had not been able to monitor e-mail activities.

F. Determined whether the IRS has considered using filters to restrict the movement of e-mail (i.e., to certain sites outside the IRS network).

G. Attempted to determine the extent of business and non-business e-mail usage by obtaining and loading a sample of Treasury Department logs into a database and analyzing the available data for e-mail sites accessed. Identified, when possible, those messages deemed non-business with specific locations. Interviewed personnel from the IRS Office of Labor Relations, IRS Data Security Staffs, and Treasury Inspector General for Tax Administration Office of Investigations to identify any instances of violations of e-mail policies resulting in misconduct.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Gerald Horn, Audit Manager
Richard Borst, Senior Auditor
David Hodge, Auditor
William Simmons, Auditor

Appendix III

Report Distribution List

Deputy Commissioner Operations C:DO
Chief Information Officer IS
Deputy Chief Information Officer IS
Director, Telecommunications IS:T
Director, Security and Privacy Oversight IS:SPO
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis M:O
Office of Management Controls CFO:A:M
Office of Chief Counsel CC
National Taxpayer Advocate TA
Audit Liaison: Chief Information Officer IS